5 Tips to Spot a **Phishing Email**

The trick is to always be alert!

Links and attachments

Be wary of suspicious links and attachments. If you're unsure, don't click! It's always better to access your account via the website directly rather than logging in through a link in the email.

Check the from address

Always check the from address, often it's easy to spot a fake but sometimes you need to take a closer look as there can be small differences such as the legit "company.name@" to the fraudulent "company-name@".

Grammar and spelling

Check for simple typos and sentences that don't make sense. Fonts and colours that don't match the brand and if the email isn't personally addressed to you, that is also a good give away that it's a phishing scam.

Is it URGENT?

Attackers like to create a sense of urgency to instil panic, as panic often makes you more likely to make a mistake. Never act impulsively, instead, you should take a step back, breathe and question the authenticity.

If you're not sure? Ask!

If in doubt, call the person emailing you or ask for a second opinion! You should also keep your anti-virus and email security up to date so it can detect potential threats in your system.

We always recommend a multi-layered approach including multi-layered cyber security support, disaster recovery solutions and user education.

For more advice on email security visit:

www.complete-it.co.uk/complete-email-security/

cit
Complete I.T.